

09/03/99
JC688 U.S. PTO

Please type a plus sign (+) inside this box → ☐

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.

192304-1035

First Named Inventor or Application Identifier

Greg B. Garrison

Title

SYSTEM AND METHOD FOR ENCRYPTING DATA MESSAGES

Express Mail Label No.

EL445741065US

APPLICATION ELEMENTS

See MPEP Chapter 600 concerning utility patent application contents

ADDRESS TO:

Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original, and a duplicate for fee processing)
2. ☒ Specification [Total Pages **26**]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R&D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure
3. ☒ Drawing(s) (35 USC d113) [Total Sheets **7**]
4. Oath or Declaration [Total Pages **2**]
a. ☐ Newly Executed (original or copy)
b. ☐ Copy from a prior application (37 CFR §1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s)
named in the prior application,
see 37 CFR §1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of
the oath or declaration is supplied under Box 4b, is considered as
being part of the disclosure of the accompanying application and is
hereby incorporated by reference therein.

6. ☐ Microfiche Computer Program (Appendix)
7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identical of above copies

ACCOMPANYING APPLICATION PARTS

8. ☐ Assignment Papers (cover sheet & Documents(s))
9. ☐ 37 CFR §3.73(b) Statement [] Power of Attorney
(when there is an assignee)
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement (IDS)/PTO-1449 [] Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. ☒ Small Entity Statement(s) [] Statement filed in prior application
(PTO/SB/09-12) Status still proper and desired
15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. ☐ Other: _____

*A new statement is required to be entitled to pay small entity fees, except where one has been filed in a prior application and is being relied upon.

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information below and in a preliminary amendment:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____
Prior application information: Examiner _____ Group / Art Unit: _____


18. CORRESPONDENCE ADDRESS

☐ Customer Number or Bar Code Label

(Insert Customer No. or Attach bar code label here)

or ☒ Correspondence address below

NAME	Jon E. Holland Thomas, Kayden, Horstemeyer & Risley, L.L.P.		
ADDRESS	100 Galleria Parkway Suite 1500		
CITY	Atlanta	STATE	Georgia
COUNTRY	U.S.A.	TELEPHONE	770-933-9500
		ZIP CODE	30339-5948
		FAX	770-951-0931

Name (Print/Type)	Jon E. Holland	Registration No. (Attorney/Agent)	41,077
Signature		Date	9/3/99

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

09/03/99
16688 U.S. PTO

4

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Garrison

Examiner: To Be Assigned

Serial No.: To Be Assigned

Group No.: To Be Assigned

Filing Date: September 3, 1999

For: SYSTEM AND METHOD FOR ENCRYPTING DATA MESSAGES

CERTIFICATE OF EXPRESS MAIL


Assistant Commissioner for Patents
BOX: Patent Application
Washington, D.C. 20231

Sir:

Enclosed for filing in the above case are the following documents:

Return Postcard
Utility Patent Application Transmittal
Fee Transmittal
Utility Patent Application including:
19 Pages of Specification
6 Pages of Claims
1 Page of Abstract
7 Pages of Formal Drawings
Unsigned Declaration
Unsigned Small Entity Statement
Check in the amount of \$416.00

Respectfully submitted,


Jon E. Holland
Registration No. 41,077

**THOMAS, KAYDEN, HORSTEMEYER
& RISLEY, L.L.P.**
100 Galleria Parkway, N.W.
Suite 1500
Atlanta, Georgia 30339-5948

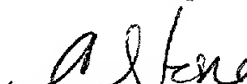
Our Docket No: 192304-1035

I hereby certify that all correspondences listed above are being deposited for delivery to the above addressee, with the United States Postal Service "**EXPRESS MAIL POST OFFICE TO ADDRESSEE**" service under 37 CFR §1.10 on the date indicated below:

The envelope has been given U.S. Postal Service "Express Mail Post Office To Addressee" Package #
EL445741065US.

Date:

September 3, 1999


Carla Bridwell Stone

Applicant or Patentee: Garrison
Serial or Patent No.: To Be Assigned
Filed or Issued: Herewith
For: **SYSTEM AND METHOD FOR ENCRYPTING DATA MESSAGES**

**VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY
STATUS (37 C.F.R. §1.9(f) AND 1.27(c)) - SMALL BUSINESS CONCERN**

I hereby declare that I am

- ☐ the owner of the small business concern identified below:
☒ an official of the small business concern empowered to act on behalf of the
concerned identified below:

NAME OF CONCERN: Westcorp Software Systems, Inc.
ADDRESS OF CONCERN: 20 Technology Parkway, Suite 200, Norcross, Georgia 30092

I hereby declare that the above-identified small business concern qualifies as a small business concern as defined in 13 CFR 121.3-18, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees under Section 41(a) and (b) of Title 35, United States Code, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third-party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed, to and remain with the small business concern identified above with regard to the invention, entitled:

SYSTEM AND METHOD FOR ENCRYPTING DATA MESSAGES

by inventor(s): Greg B. Garrison

described in

- ☒ the specification filed herewith.
☐ application serial no. _____, filed _____.
☐ patent no. _____, issued _____.

If the rights held by the above-identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

*NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities (37 CFR 1.27)

NAME: _____

ADDRESS: _____

☐ INDIVIDUAL ☐ SMALL BUSINESS CONCERN ☐ NONPROFIT ORGANIZATION

NAME: _____

ADDRESS: _____

☐ INDIVIDUAL ☐ SMALL BUSINESS CONCERN ☐ NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any changes in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small business entity is no longer appropriate. (37 CFR 1.28(b)).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING: Charles B. West

TITLE OF PERSON OTHER THAN OWNER: Chairman

ADDRESS OF PERSON SIGNING: 20 Technology Parkway, Suite 200, Norcross, Georgia 30092

SIGNATURE _____

Date _____

SYSTEM AND METHOD FOR ENCRYPTING DATA MESSAGES

BACKGROUND OF THE INVENTION

5

FIELD OF THE INVENTION

The present invention generally relates to encryption techniques and, in particular, to a system and method for encrypting data communicated between two computers remotely located from each other.

10

RELATED ART

With the introduction of the Internet and other technological advances, computers now have the capability of communicating across vast distances. However, communication over vast distances presents certain security issues in some applications that utilize sensitive or private information. In this regard, it is often difficult to prevent an unauthorized user, sometimes referred to as a "hacker," from gaining access to a portion of a data path connecting two computers that are remotely located from each other. Therefore, it is possible for a hacker to intercept at least some of the messages communicated during a data session between the two computers.

20

As a result, encryption techniques have been developed to prevent hackers from deciphering messages that have been intercepted. Most encryption techniques utilize a key or keys that translate (*i.e.*, encrypt) the data of a message into an unrecognizable form before transmission. The intended recipient at some point is provided with a key or keys that may be used to translate (*i.e.*, decrypt) the unrecognizable message into a recognizable

form so that the message can be read and processed by the recipient. Therefore, even if a hacker intercepts a message, the hacker should be unable to read the message, because the hacker should not have the key or keys needed to properly decrypt the message.

However, not all encryption techniques afford the same quality of protection from hackers. In this regard, it is possible for some hackers to determine (*i.e.*, “break”) the algorithm used to encrypt an intercepted message and, therefore, to decipher the contents of the intercepted message. Some encryption techniques utilize a more complex encryption scheme, which is generally more difficult to break than a less complex encryption scheme. However, more complex encryption schemes generally take longer to encrypt and decrypt and, therefore, reduce the throughput for the data session.

For example, two commonly used encryption techniques are data encryption standard (DES) and Rivest-Shamir-Adleman (RSA) encryption. RSA encryption is usually more difficult to break than DES encryption, but RSA encryption causes a significant reduction in throughput as compared to DES encryption. Accordingly, in applications in which large amounts of data need to be transmitted, DES encryption is often selected over RSA encryption, even though DES encryption is viewed by many as a less secure encryption technique.

Thus, a heretofore unaddressed need exists in the industry for a highly secure encryption scheme that minimally impacts throughput.

SUMMARY OF THE INVENTION

The present invention overcomes the inadequacies and deficiencies of the prior art as discussed herein. In general, the present invention provides a system and method for encrypting data communicated between two computers. The encryption scheme used to
5 encrypt the data provides a high degree of security without a relatively significant effect to throughput.

In accordance with the present invention a first computer encrypts a data portion of a message via a first encryption technique before transmitting the message to a second computer. The first computer also includes information associated with the first encryption
10 technique in a header of the message and encrypts the header via a second encryption technique. The second computer receives the data message and decrypts the header. The second computer then utilizes the information in the header that is associated with the first encryption technique to decrypt the data portion.

In accordance with another feature of the present invention, the information
15 associated with the first encryption technique identifies the first encryption technique and/or identifies an encryption key used to encrypt the data portion. It is possible for either the first encryption technique and/or the encryption key to be randomly selected by the first computer.

The present invention can also be viewed as providing a method for transmitting
20 messages between computers. The method can be broadly conceptualized by the following steps: defining a data portion of a first data message; encrypting the data portion of the first data message via a first encryption technique; defining a header of the first data message, the header of the first data message including information associated with the

first encryption technique; encrypting the header of the first data message via a second encryption technique; and transmitting the first data message subsequent to the encrypting steps.

Other features and advantages of the present invention will become apparent to one skilled in the art upon examination of the following detailed description, when read in conjunction with the accompanying drawings. It is intended that all such features and advantages be included herein within the scope of the present invention, as is defined by the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention can be better understood with reference to the following drawings. The elements of the drawings are not necessarily to scale relative to each other, emphasis instead being placed upon clearly illustrating the principles of the invention. Furthermore, like reference numerals designate corresponding parts throughout the several views.

FIG. 1 is a block diagram illustrating a communication system in accordance with the present invention.

FIG. 2 is a block diagram illustrating a client computer system depicted in FIG. 1.

FIG. 3 is a block diagram illustrating a server computer system depicted in FIG. 1.

FIG. 4 is a block diagram illustrating an exemplary data message that may be transmitted by the communication system depicted in FIG. 1.

FIG. 5 is a flow chart illustrating the architecture and functionality of the communication system depicted in FIG. 1.

FIG. 6 is a flow chart illustrating a more detailed view of a portion of the flow chart depicted in FIG. 5.

FIG. 7 is a flow chart illustrating a more detailed view of another portion of the flow chart depicted in FIG. 5.

5 FIG. 8 is a flow chart illustrating a more detailed view of another portion of the flow chart depicted in FIG. 5.

DETAILED DESCRIPTION OF THE INVENTION

FIG. 1 depicts a communication system 10 illustrating the principles of the present invention. Referring to FIG. 1, a client 14 is configured to communicate with a server 17 via communications network 18. The client 14 is preferably a computer system located remotely from the server 17, which is preferably a computer system as well. As used herein, the terms “remotely located” or “remote location” shall refer to a location separated from the premises of a server 17 by an unsecure connection. An unsecure connection is any connection accessible by a hacker or unauthorized user. Examples of unsecure connections are, but are not limited to, Internet connections, publicly switched telephone network (PSTN) connections, cellular connections *etc.* The communications network 18 can comprise any conventional communications network or combinations of networks such as, for example (but not limited to), the PSTN, a cellular network, *etc.* Furthermore, the communications network 18, along with the client 14 and server 17, may employ any protocol or combinations of protocols suitable for communicating information between the client 14 and the server 17.

The server 17 is preferably associated with and connected to a database system 19 having at least one database 20a or 20b. The database system 19 is preferably located on a premises of the server 17, and information stored within each database 20a and 20b can be accessed by the server 17 through known techniques. Copending U.S. patent application
5 entitled "System and Method for Encrypting a Data Session Between a Client and a Server," assigned Serial No. 09/146,264, and filed on September 3, 1998, which is incorporated herein by reference, describes techniques that may be employed by server 17 to retrieve data from database system 19.

Referring now to FIG. 2, the client 14 preferably includes a control system 21 for
10 controlling the operation of the client 14. The client control system 21 can be implemented in hardware, software, or a combination thereof. In the preferred embodiment, the client control system 21 along with its associated methodology is preferably implemented in software and stored in memory 22 of the client 14. Note that the client control system 21 can be stored and transported on any computer-readable medium for use by or in connection with
15 a computer-readable system or method. In the context of this document, a computer-readable medium is an electronic, magnetic, optical, or other physical device or means that can contain or store a computer program for use by or in connection with a computer-related system or method. As an example, the client control system 21 may be magnetically stored and transported on a conventional portable computer diskette.

20 The preferred embodiment of the client 14 of FIG. 2 comprises one or more conventional processing elements 25, such as a digital signal processor (DSP), that communicate to and drive the other elements within the client 14 via a local interface 26, which can include one or more buses. Furthermore, an input device 28, for example, a

keyboard or a mouse, can be used to input data from a user of the client 14, and a screen display 29 or a printer 31 can be used to output data to a user. A disk storage mechanism 32 can be connected to the local interface 26 to transfer data to and from a nonvolatile disk (*e.g.*, magnetic, optical, *etc.*). The client 14 can be connected to a network interface 33 that allows the client 14 to exchange data with a network 34.

Furthermore, as shown by FIG. 3, the server 17 preferably comprises a computer system similar to the client 14. A control system 41 associated with the server 17 preferably controls the operations of the server 17. The server control system 41 may be implemented in hardware, software, or a combination thereof. In the preferred embodiment, the server control system 41 along with its associated methodology is preferably implemented in software and stored in memory 42 of the server 17. Note that the server control system 41 can be stored and transported on any computer-readable medium for use by or in connection with a computer-readable system or method.

Similar to the client 14, the preferred embodiment of the server 17 comprises one or more conventional processing elements 45, such as a digital signal processor (DSP), that communicate to and drive the other elements within the server 17 via a local interface 46, which can include one or more buses. Furthermore, an input device 48, for example, a keyboard or a mouse, can be used to input data from a user of the client 14, and a screen display 49 or a printer 51 can be used to output data to a user. A disk storage mechanism 52 can be connected to the local interface 46 to transfer data to and from a nonvolatile disk (*e.g.*, magnetic, optical, *etc.*). The server 17 can be connected to a network interface 53 that allows the server 17 to exchange data with a network 54.

Referring again to FIG. 1, the client 14 is configured to establish communication with the server 17 through any suitable technique known in the art. For example, the client 14 can be connected to a modem 61 which establishes communication with a modem 63 connected to the server 17. Once communication between the modems 61 and 63 is established, the client 14 can communicate with the server 17 via communications network 18 and modems 61 and 63. However, one skilled in the art should realize that communication devices other than modems 61 and 63 may be used to establish communication between client 14 and server 17.

After a data connection is established between the client 14 and the server 17, the client 14 and the server 17 are configured to establish a first type of encryption scheme, such as the well-known Diffie-Hellman encryption scheme, for example, although other types of encryption schemes may be established. In this regard, the server 17 is configured to generate Diffie-Hellman parameters and to transmit the Diffie-Hellman parameters to the client 14. The client 14, through well known techniques, is designed to generate a public key (hereinafter referred to as "the client's Diffie-Hellman public key") based on the received Diffie-Hellman parameters. The client 14 then transmits this public key to the server 17, which is configured to utilize the client's Diffie-Hellman public key and the Diffie-Hellman parameters to generate a public key (hereinafter referred to as "the server's Diffie-Hellman public key") and a Diffie-Hellman key, which can be utilized in conjunction with a Diffie-Hellman public key to decrypt data.

After generating the server's Diffie-Hellman public key, the server 17 is configured to transmit the server's Diffie-Hellman public key to the client 14. Based on the server's Diffie-Hellman public key and the Diffie-Hellman parameters previously transmitted to the

client 14, the client 14 is designed to discover the Diffie-Hellman key. Therefore, at this point, both the client 14 and the server 17 are aware of the Diffie-Hellman key that is to be used for the data session and are aware of the server's Diffie-Hellman public key and the client's Diffie-Hellman public key. As a result, the client 14 and the server 17 may encrypt
5 and decrypt data communicated therebetween via conventional Diffie-Hellman encryption techniques.

In the preferred embodiment, both the client 14 and the server 17 are respectively associated with a pair of public and private keys that may be used to encrypt and decrypt data according to conventional public/private key pair encryption techniques, such as
10 Rivest-Shamir-Adleman (RSA), for example. In this regard, the client 14 is configured to transmit the client's RSA public key to the server 17, and the server 17 is configured to transmit the server's RSA public key to the client 14. To enhance security of the data communicated by the system 10, both the client's RSA public key and the server's RSA public key are encrypted via Diffie-Hellman encryption techniques before transmission.
15 Once the server 17 has received and decrypted the client's RSA public key and the client 14 has received and decrypted the server's RSA public key, the client 14 and the server 17 may encrypt and decrypt future messages according to RSA encryption techniques.

After exchanging the RSA public keys, the client 14 and the server 17 preferably encrypt all messages transmitted therebetween via RSA encryption techniques. However,
20 RSA encryption techniques typically slow data transfer considerably, and completely encrypting each of the messages communicated between the client 14 and the server 17 via RSA encryption techniques or other types of highly secure encryption techniques may significantly decrease the throughput of the system 10. Therefore, instead of completely

encrypting each message via RSA encryption techniques, the client 14 and the server 17 are configured to encrypt only a portion of each message via RSA encryption techniques (or another type of high security encryption technique) and to encrypt the remaining portion of each message with a faster type of encryption technique.

5 FIG. 4 shows an exemplary data message 101 that is communicated between client 14 and server 17. In the preferred embodiment, the message 101 is a data packet in accordance with transmission control protocol/internet protocol (TCP/IP) so that the message may be communicated via the Internet or other types of networks that utilize TCP/IP. However, the message 101 may be compatible with other types of protocols in
10 other embodiments.

 The message 101 includes a data portion 103, a decryption header 105, and a routing header 107. The routing header 107 includes routing information, such as a destination address, for example, required by the network 18 (FIG. 1) to route the message 101 to the intended recipient (*e.g.*, either client 14 or server 17). Therefore, the routing
15 header 107 should be unencrypted to allow components of the network 18 to read and understand the routing information within the routing header 107.

 The data portion 103 includes data that is to be received and processed by either the client 14 or server 17 through conventional techniques. For example, the data portion 103 may include data defining a request to retrieve data or may include data that has been
20 retrieved in response to a request to retrieve data. The data portion 103 is preferably encrypted via any conventional encryption technique. For example, the data portion 103 may be encrypted via well-known data encryption standard (DES) techniques, which utilize

the same encryption key to encrypt and decrypt data. However, other types of encryption techniques may be used to encrypt the data portion 103 in other embodiments.

To increase the security of the messages 101, each data portion 103 is preferably encrypted with a randomly selected encryption technique or with a randomly selected encryption key. Furthermore, the decryption header 105 preferably includes sufficient data to enable the recipient (*e.g.*, client 14 or server 17) of the message 101 to decrypt the data portion 103. For example, when the data portion 103 has been encrypted via DES encryption techniques, as described above, the decryption header 105 preferably includes information indicating that DES encryption techniques have been used to encrypt the data portion 103 and preferably includes the DES key used to encrypt the data portion 103. As a result, the recipient of the message 101 is able to decrypt the data portion 103 using the information included in the decryption header 105.

To ensure that an unauthorized user cannot use the information in decryption header 105 to decrypt the data portion 103 in the event that the message 101 is intercepted by an unauthorized user, the decryption header 105 is preferably encrypted via a different and preferably more secure encryption technique, such as RSA encryption, for example. Therefore, upon receiving the message 101, the recipient of the message 101 is configured to decrypt the decryption header 105 via RSA encryption techniques, and based upon the information decrypted from the decryption header 105, the recipient is configured to decrypt the data portion 103.

It should be noted that because the decryption header 105 of message 101 includes sufficient data for the recipient to decrypt the data portion 103, the encryption technique and/or the encryption key used to encrypt the data portion 103 of different messages 101

transmitted by client 14 and/or server 17 may be changed for each message 101 communicated during the data session. For example, the client 14 or server 17 may encrypt the data portion 103 of each message respectively transmitted by the client 14 or server 17 in the data session with a randomly selected encryption key, such that the data portions 103 of different messages 101 are encrypted with different encryption keys. Also, the client 14 or server 17 may encrypt the data portion 103 of each message 101 respectively transmitted by the client 14 or server 17 via a randomly selected encryption technique, such that the encryption techniques used to encrypt the data portions 103 of different messages 101 changes during the data session.

10 As a result, if an unauthorized user intercepts the messages 101 of the data session and is able to decipher the data portion 103 of one of the messages 101, the data portions 103 of the other methods should still be secure. In other words, breaking the encryption of the data portion 103 of one of the messages 101 does not enable an unauthorized user to decipher the data portions 103 of other messages 101. Therefore, as long as the
15 unauthorized user is unable to break the encryption scheme of the decryption header 105, which can be encrypted with a relatively strong encryption scheme, then the overall integrity of the data session should be preserved. Consequently, to maximize throughput, a user can choose to encrypt the data portion 103 with relatively fast encryption techniques over slower but more secure encryption techniques without significantly jeopardizing the
20 security of the data transmitted by the data portions 103.

To further increase the security of the message 101, various other security features may be utilized. For example, a hash may be inserted into each data message 101 to indicate via conventional techniques whether the data within the message 101 has changed

since the message was originally transmitted. In other words, the hash indicates whether the data within the message 101 has been altered by an unauthorized user. Therefore, a recipient of the message 101 may analyze the hash via conventional hashing techniques to determine whether the data has been altered by an unauthorized user. If the data has been so altered, the recipient is preferably configured to ignore the message 101.

In addition, the decryption header 105 may also include an authorization indicator to verify that the message 101 has been transmitted from a reliable source. For example, the client 14 may transmit a message 101 to the server 17 requesting the server 17 to retrieve certain data. The client 14 is preferably configured to insert an authorization indicator, which can be any number or other type of value known to the client 14. In this example, the server 17 is configured to retrieve data in response to the message 101 transmitted by the client 14 and to transmit the retrieved data to the client 14 via another message 101. The server 17 is preferably configured to insert the authorization indicator read from the request transmitted by the client 14 into the decryption header 105 of the message 101 transmitted by the server 17. Therefore, upon receiving the message 101 from the server 17, the client 14 can verify that the message 101 is from the server 17 when the client 14 locates the authorization indicator in the message 101. If the client 14 is unable to locate the authorization indicator in the message 101 received by the client 14, then the client 14 is configured to assume that the message 101 has been transmitted from an unreliable source and is configured to ignore the received message 101. It should be noted that security features other than the ones previously described may be implemented by the client 14 and/or server 17 without departing from the principles of the present invention.

OPERATION

The preferred use and operation of the communication system 10 and associated methodology are described hereafter.

5 Initially, client 14 establishes a communication connection with server 17 via network 18 through conventional techniques, as shown by block 125 of FIG. 5. The client 14 and server 17 then use Diffie-Hellman key exchange in block 128 to obtain the client's Diffie-Hellman public key, the server's Diffie-Hellman public key, and the Diffie-Hellman key.

10 In this regard, once the communication connection is established between the client 14 and the server 17, the server 17 generates Diffie-Hellman parameters and transmits the Diffie-Hellman parameters to client 14, as depicted by a block 131 of FIG. 6. Through conventional techniques, the client 14 generates the client's Diffie-Hellman public key based on the Diffie-Hellman parameters transmitted from the server 17. As shown by
15 block 135, the client 14 transmits the client's Diffie-Hellman public key to the server 17. The server 17 uses this public key along with the Diffie-Hellman parameters generated in block 131 to generate the server's Diffie-Hellman public key, as depicted by block 137. The server 17 then transmits the server's Diffie-Hellman public key to the client 14 in block 139. As shown by block 142, the client 14 generates the Diffie-Hellman key based on the
20 server's Diffie-Hellman public key and based on the Diffie-Hellman parameters transmitted in block 131. Note that the Diffie-Hellman key generated in block 142 should match the Diffie-Hellman key generated in block 131.

After performing block 128, both the client 14 and the server 17 should have sufficient information to perform conventional Diffie-Hellman encryption and decryption. Referring again to FIG. 5, the client 14 preferably encrypts the client's RSA public key via Diffie-Hellman encryption and transmits this key to the server 17 in block 146. Likewise,
 5 the server 17 preferably encrypts the server's RSA public key via Diffie-Hellman encryption and transmits this key to the client 14, as shown by block 149. After performing block 149, the client 14 and the server 17 should have sufficient information for performing RSA encryption and decryption.

Assume for illustrative purposes, that the client 14 is to transmit a retrieval request
 10 (*i.e.*, a request to retrieve data) to server 17. In this example, the client 14 inserts the data defining the retrieval request into the data portion 103 of a message 101 and encrypts the data portion 103 before transmitting the message 101 to server 17, as shown by block 154.

In performing block 154, the client 14 defines the data portion 103 of a message
 101 with the retrieval request, as depicted by block 159 of FIG. 7. In other words, the
 15 client 14 includes data in the data portion 103 that defines the retrieval request. The client 14 then randomly selects an encryption scheme and encrypts the data portion 103 with the selected encryption scheme, as shown by blocks 161 and 163 of FIG. 7. The encryption scheme selected by the client 14 in block 161 should be compatible with server 17. In other words, the server 17 should be familiar with the encryption scheme so that the server
 20 17 can decrypt the message 101.

To ensure that the server 17 is compatible with the selected encryption scheme, the server 17 (prior to block 161) preferably transmits a list of encryption schemes that the client 14 may choose from. For example, the server 17 may transmit this list to the client

14 in block 131 (FIG. 6) along with the Diffie-Hellman parameters. The list transmitted by the server 17 may also include limitations or other information associated with the encryption schemes in the list. For example, the list may include data indicating the maximum length of an encryption key that may be used to encrypt data. Moreover, the client 14 should be aware of which encryption schemes are compatible with server 17 and can select any encryption scheme compatible with server 17 in block 161 of FIG. 7.

In selecting the encryption scheme in block 161, the client 14 may also randomly select an encryption key with which to encrypt the retrieval request according to the selected encryption schemes. Furthermore, as shown by block 164, the client 14 includes information in the decryption header 105 that enables the server 17 to decrypt the data portion 103, which is encrypted according to the encryption scheme selected in block 161. For example, in the preferred embodiment, the client 14 includes information in the decryption header 105 indicating which type of encryption scheme and which encryption key was selected in block 161. However, in other embodiments, other types of information may be included in the decryption header 105 to enable the server 17 to decrypt the data portion 103.

After defining the decryption header 105, the client 14 (as shown by block 172) encrypts the decryption header 105 via RSA encryption (*i.e.*, utilizing the server's RSA public key transmitted to the client 14 in block 149). Then, in block 177, the client 14 transmits the encrypted message 101 to the server 17.

In block 181 of FIG. 5, the server 17 receives and decrypts the message 101 transmitted by the client 14 in block 154. Referring to FIG. 8, the server 17 receives the message 101 in block 182 and, as shown by block 183, decrypts the decryption header 105

using RSA decryption (*i.e.*, utilizing the client's RSA public key transmitted to the server 17 and block 146). Based on the information contained in the decryption header 105, the server 17 determines which encryption scheme and which encryption key was used by the client 14 to encrypt the data in data portion 103. Therefore, by reading the decryption
 5 header 105, the server 17 should have sufficient information to decrypt the data portion 103. Accordingly, the server 17 decrypts the data portion 103 in block 186 and reads the retrieval request included in the data portion 103. The server 17 then processes the retrieval request according to conventional techniques.

In this regard, the server 17 retrieves data from the database system 19 in response
 10 to the retrieval request. As shown by block 201 of FIG. 5, blocks 154 and 181 are repeated for each data message transmitted between client 14 in server 17. Therefore, the server 17 performs blocks 154 and 181 to transmit the data retrieved from database system 19. However, because the encryption scheme and the encryption key is randomly selected in block 161 (FIG. 7), it is not likely that the server 17 will encrypt the message 101
 15 transmitted to client 14 with the same encryption scheme and/or encryption key used by the client 14 in encrypting the retrieval request.

To ensure that the client 14 can read the message 101 transmitted by the server 17, the server 17 preferably selects an encryption scheme in block 161 (FIG. 7) that is compatible with the client 14. Therefore, the server 17 preferably maintains a list of
 20 encryption schemes used by client 14 in transmitting messages 101 to server 17. The server 17 in block 161 only selects encryption schemes from this list maintained by the server 17. As a result, the server 17 should only encrypt messages 101 with encryption schemes compatible with the client 14.

If desired, other messages 101 may be transmitted between the client 14 and server 17. For each message 101 transmitted, blocks 154 and 181 are performed by the transmitting device (*i.e.*, either client 14 or server 17). As a result, the encryption key used to encrypt the data portion 103 of the messages 101 changes during the data session.

5 Therefore, a fast type of encryption may be used to encrypt the data portion 103 without significantly jeopardizing the security of the data in the data portion 103. In this regard, even if the encryption of the data portion 103 of one of the messages 101 is broken by a hacker, the security of the other messages 101 is not jeopardized, since the data portions 103 of the other messages 101 are encrypted with different encryption techniques and/or
10 encryption keys. The security of each of the messages 101 is compromised only if the encryption of the decryption header 105 is broken. Therefore, by encrypting the decryption header 105 with a relatively secure encryption technique, the security level of the messages 101 can be maximized without significantly affecting the transmission speed of the messages 101. Once each message 101 of a data session has been communicated, the
15 connection between client 14 and server 17 can be terminated, as shown by block 204.

It should be noted that RSA and DES encryption have been described hereinabove for the purposes of illustration only. Encryption schemes other than those described herein may be used to encrypt the decryption header 105 and/or the data portion 103 without departing from the principles of the present invention.

20 It should be emphasized that the above-described embodiments of the present invention, particularly, any “preferred” embodiments, are merely possible examples of implementations, merely set forth for a clear understanding of the principles of the invention. Many variations and modifications may be made to the above-described

embodiment(s) of the invention without departing substantially from the spirit and principles of the invention. All such modifications and variations are intended to be included herein within the scope of the present invention and protected by the claims.

CLAIMS

Now, therefore, the following is claimed:

- 1 1. A system for securely transmitting data messages, comprising:
- 2 a first computer configured transmit a data message, said data
- 3 message having a header and a data portion, said first computer
- 4 configured to encrypt said data portion via a first encryption
- 5 technique and to encrypt said header via a second encryption
- 6 technique, said first computer further configured to include
- 7 information associated with said first encryption technique in said
- 8 header; and
- 9 a second computer configured to receive said first data message
- 10 and to decrypt said header, said second computer further configured
- 11 to decrypt said data portion based on said information included in
- 12 said header.
- 1 2. The system of claim 1, wherein said information associated with said first
- 2 encryption technique identifies said second encryption technique.
- 1 3. The system of claim 1, wherein said second encryption technique includes
- 2 RSA encryption.

- 1 4. The system of claim 3, wherein said first encryption technique includes
2 DES encryption.
- 1 5. The system of claim 1, wherein said first computer transmits a public key
2 to said second computer, and wherein said second computer utilizes said public key
3 to decrypt said header.
- 1 6. The system of claim 5, wherein said first computer is configured to
2 encrypt said public key before transmitting said public key to said second computer.
- 1 7. The system of claim 1, wherein said information associated with said first
2 encryption technique identifies an encryption key used by said first computer to
3 encrypt said data portion.
- 1 8. The system of claim 7, wherein said first computer randomly selects said
2 encryption key.
- 1 9. The system of claim 1, wherein said second computer is configured to
2 transmit a list of encryption techniques to said first computer and said first
3 computer is configured to select said first encryption technique from said list.

- 1 10. The system of claim 9, wherein said first computer randomly selects said
2 first encryption technique from said list.
- 1 11. A system for transmitting messages, comprising:
2 means for defining a data portion of a data message;
3 means for encrypting said data portion via a first encryption technique;
4 means for defining a header of said data message, said header including
5 information associated with said first encryption technique;
6 means for encrypting said header via a second encryption technique; and
7 means for transmitting said message.
- 1 12. A method for transmitting messages, comprising the steps of:
2 defining a data portion of a first data message;
3 encrypting said data portion of said first data message via a first
4 encryption technique;
5 defining a header of said first data message, said header of said first data
6 message including information associated with said first encryption
7 technique;
8 encrypting said header of said first data message via a second encryption
9 technique; and
10 transmitting said first data message subsequent to said encrypting steps.

- 1 13. The method of claim 12, further comprising the steps of:
2 receiving a list of encryption techniques; and
3 randomly selecting said first encryption technique from said list.
- 1 14. The method of claim 12, wherein said first encryption technique includes RSA
2 encryption.
- 1 15. The method of claim 14, wherein said second encryption technique includes DES
2 encryption.
- 1 16. The method of claim 12, wherein said encrypting said data portion step includes
2 the step of encrypting said data portion of said first data message with an
3 encryption key, said method further comprising the step of including said
4 encryption key in said header of said first data message.
- 1 17. The method of claim 16, further comprising the step of randomly selecting said
2 encryption key.

- 1 18. The method of claim 12, further comprising the steps of:
- 2 receiving said first data message transmitted in said transmitting step;
- 3 decrypting said header of said first data message; and
- 4 decrypting said data portion of said first data message based on said
- 5 information included in said header of said first data message.
- 1 19. The method of claim 18, further comprising the step of identifying said first
- 2 encryption technique via information included in said header of said first data
- 3 message.
- 1 20. The method of claim 18, further comprising the steps of:
- 2 transmitting a public key; and
- 3 decrypting said header of said first data message based on said public key.
- 1 21. The method of claim 20, further comprising the step of encrypting said public key
- 2 before said transmitting a public key step.

1 22. The method of claim 12, further comprising the steps of:
2 defining a data portion of a second data message;
3 encrypting said data portion of said second data message via a third
4 encryption technique;
5 defining a header of said second data message, said header of said second
6 data message including information associated with said third
7 encryption technique;
8 encrypting said header of said second data message via said second
9 encryption technique; and
10 transmitting said second data message.

1 23. The method of claim 22, further comprising the step of randomly selecting said
2 first and third encryption techniques.

1 24. The method of claim 23, further comprising the steps of:
2 receiving said second message;
3 decrypting said header of said second message; and
4 decrypting said data portion of said second message based on said
5 information included in said header of said second message.

ABSTRACT OF THE DISCLOSURE

Data messages transmitted between computers are encrypted to provide a high level of security, yet the throughput of the encrypted data is minimally affected. In this regard, a first computer encrypts a data portion of a message via a first encryption technique before
5 transmitting the message to a second computer. The first computer also includes information associated with the first encryption technique in a header of the message and encrypts the header via a second encryption technique, which preferably is a highly secure encryption technique. The second computer receives the data message and decrypts the header. The second computer then utilizes the information in the header that is associated
10 with the first encryption technique to decrypt the data portion.

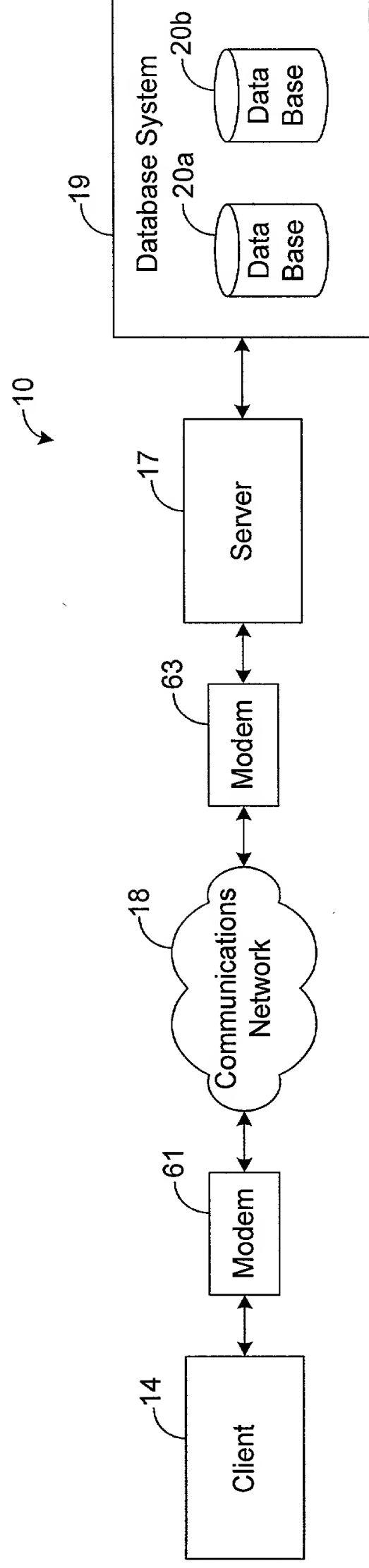


Fig. 1

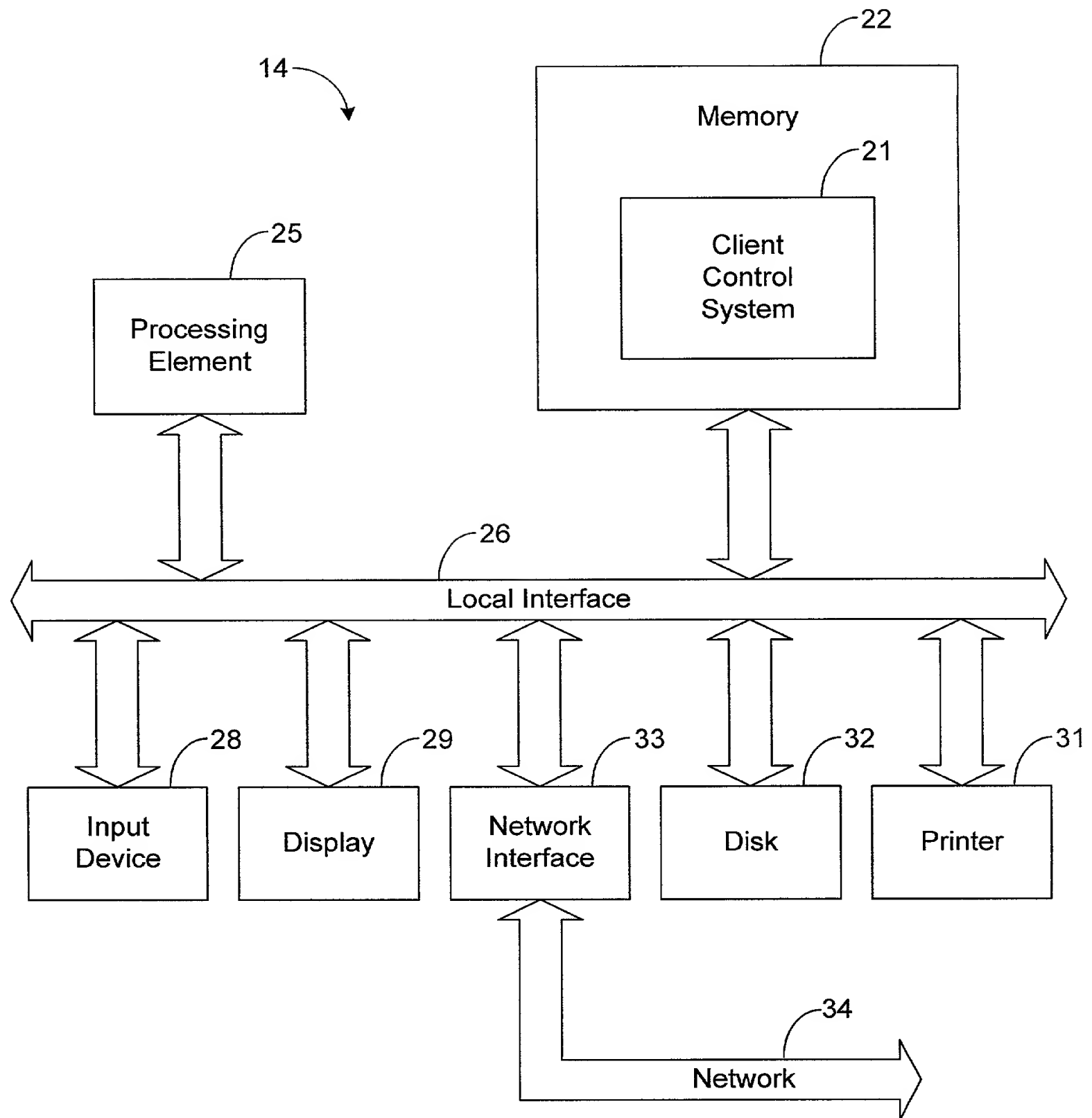


Fig. 2

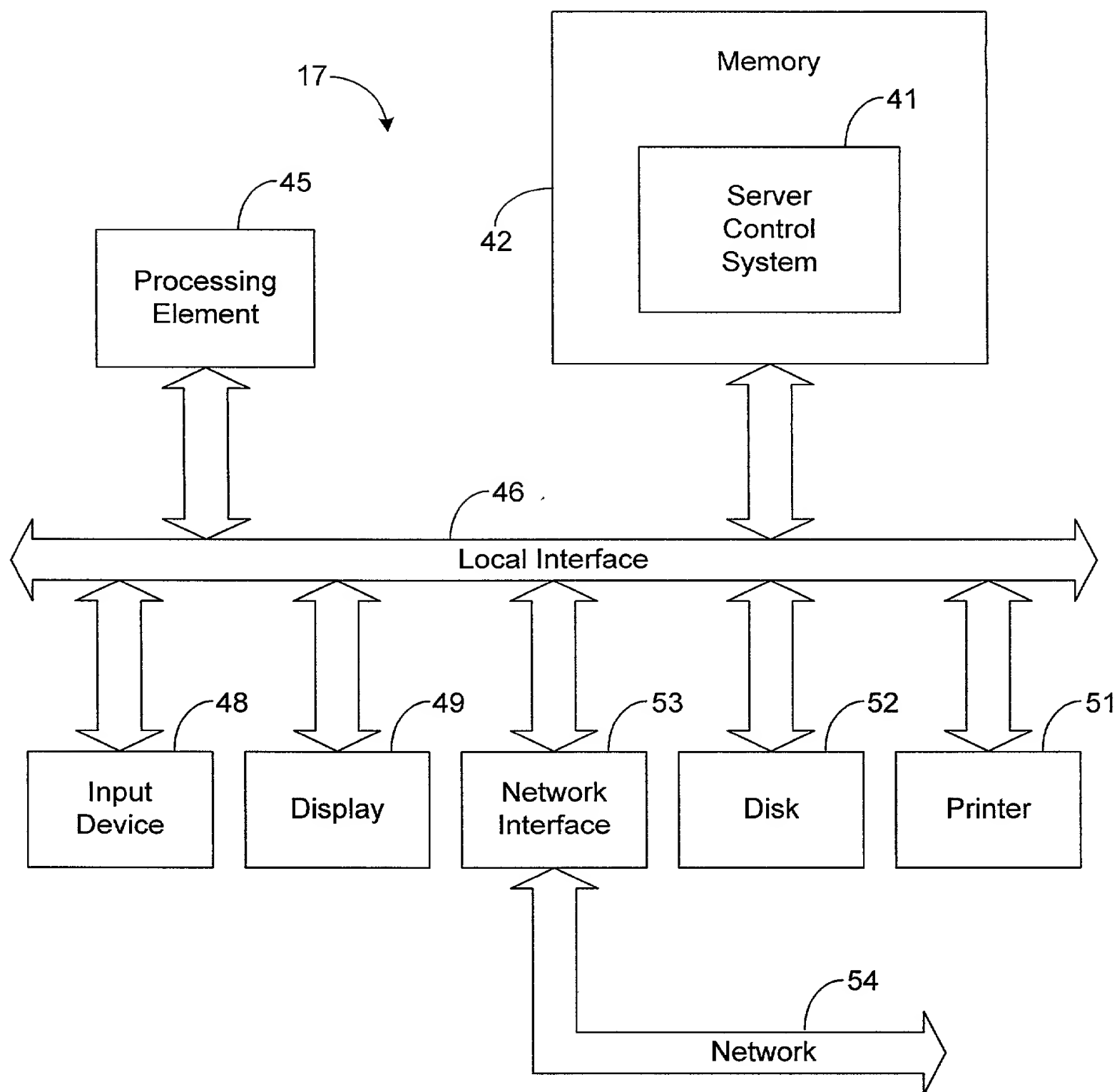


FIG. 3

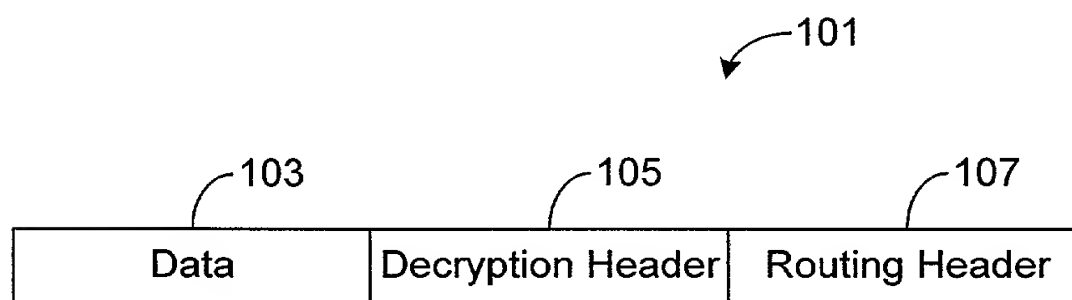


FIG. 4

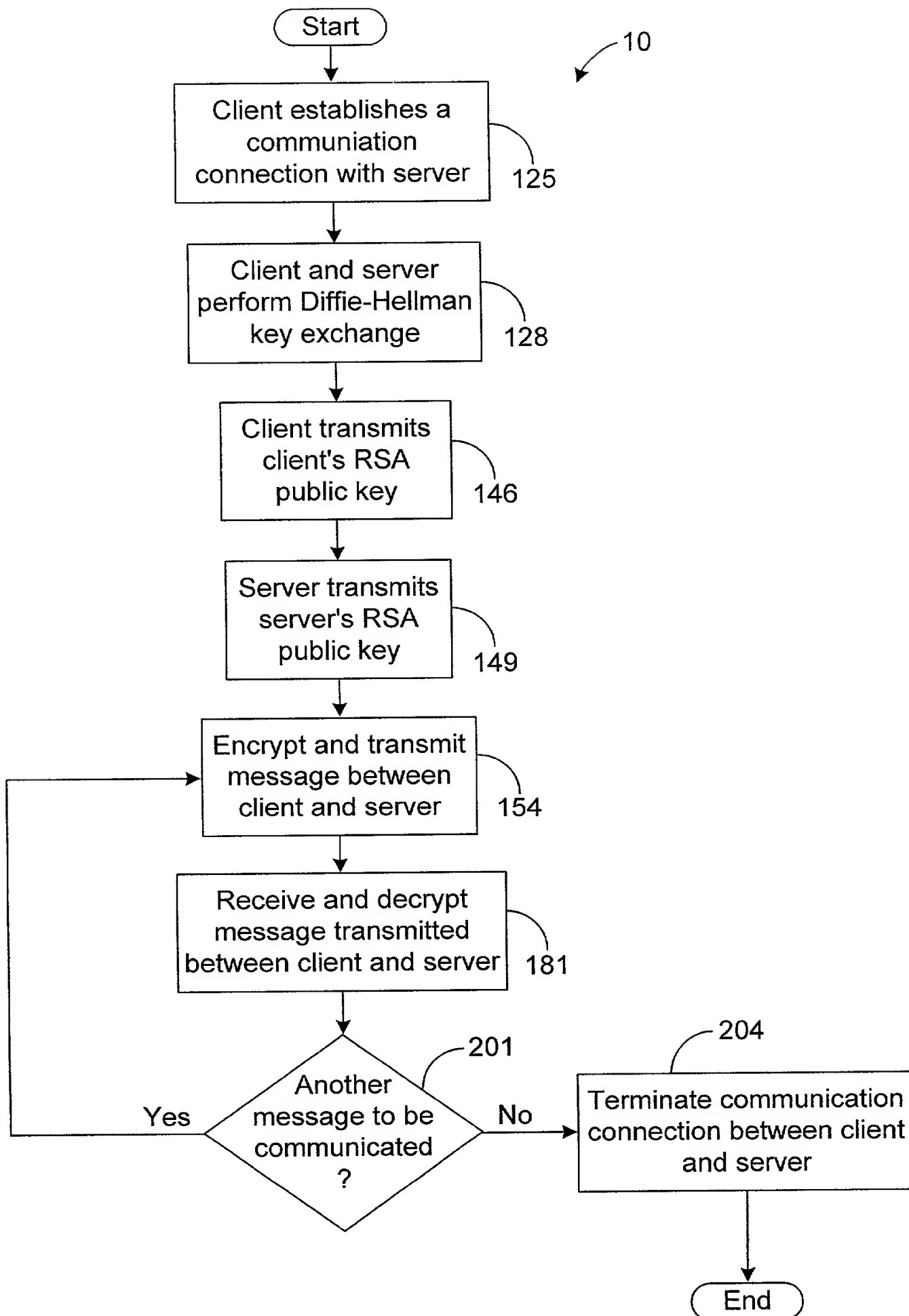


FIG. 5

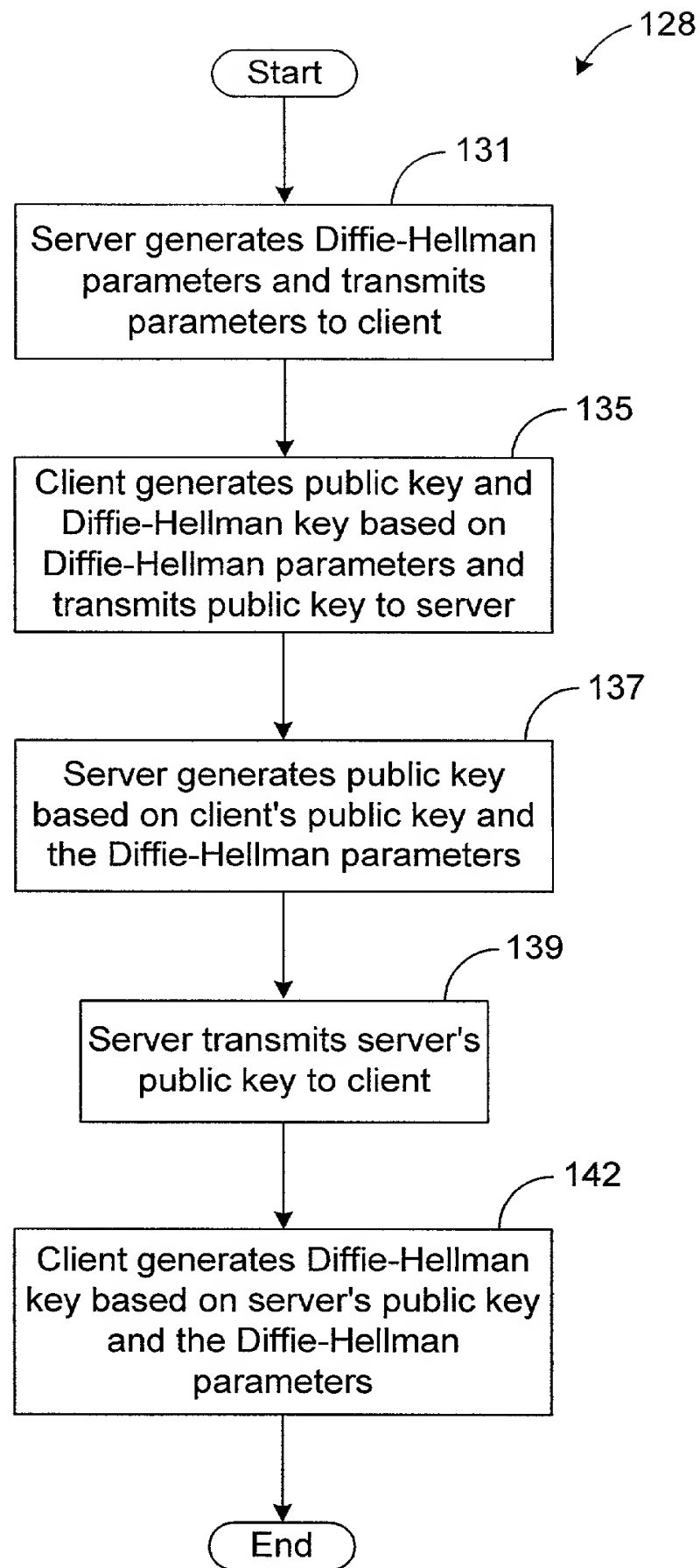


FIG. 6

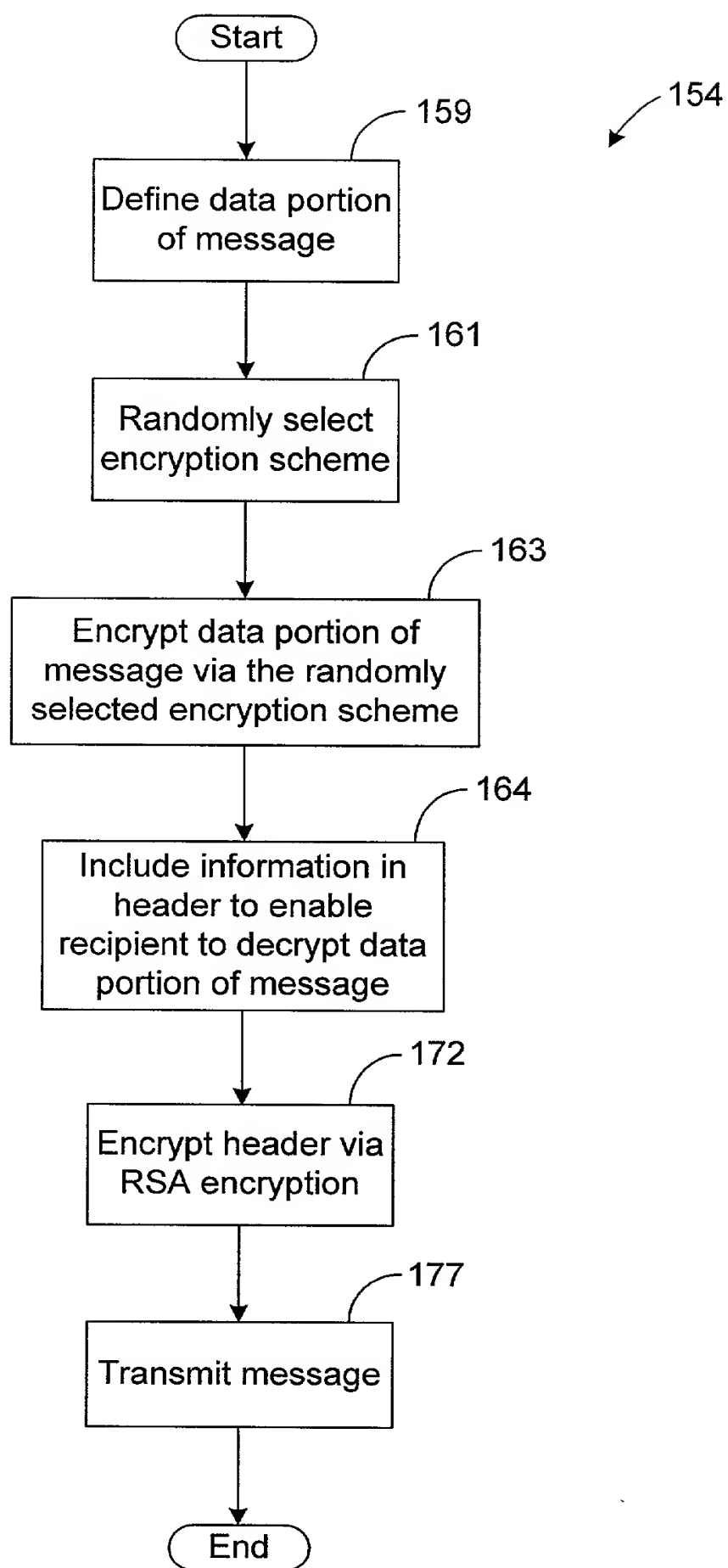


FIG. 7

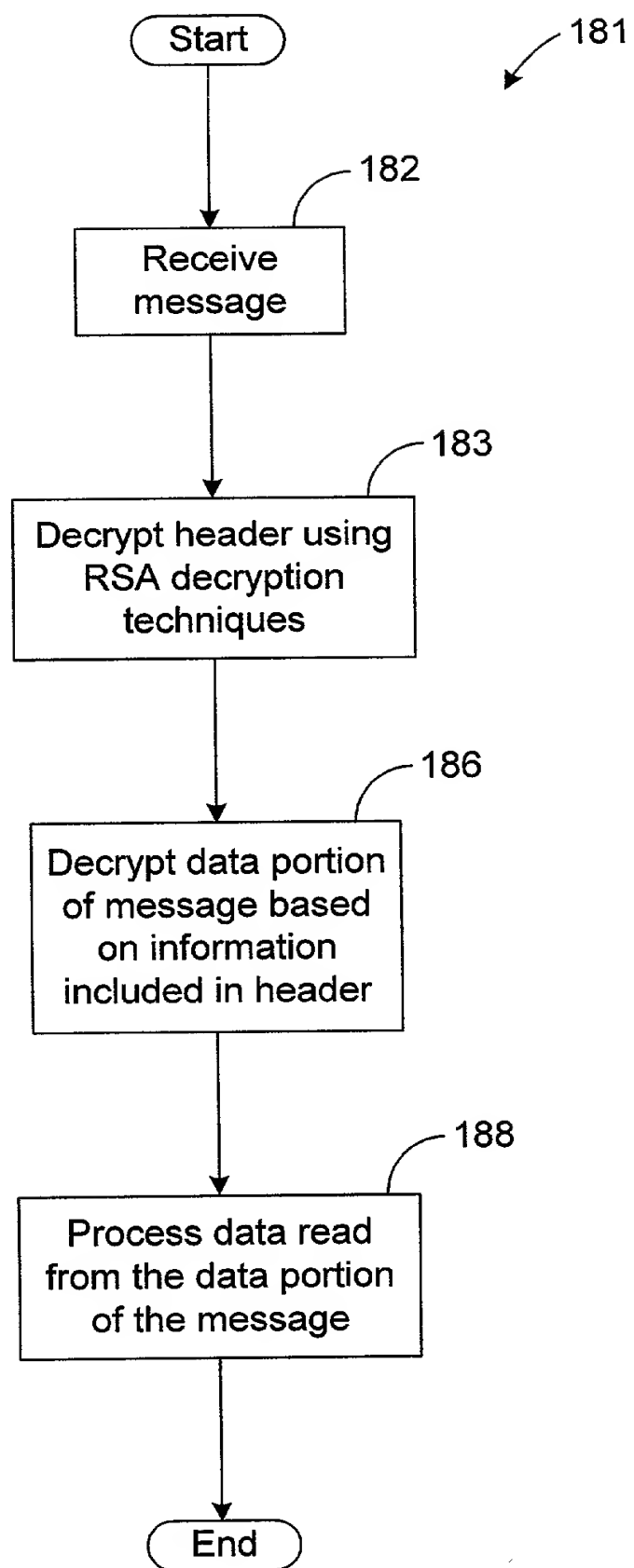


FIG. 8

DECLARATION FOR PATENT APPLICATION

Attorney Docket No: **192304-1035**

As the below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **SYSTEM AND METHOD FOR ENCRYPTING DATA MESSAGES**, the specification of which:

- ☒ is attached hereto.
- ☐ was filed on ___ as Application Serial No. ___.
- ☐ was filed on ___ under U.S. Express Mail No. ___.
- ☐ is set forth in PCT International Application No. ___;
filed on ___ and as amended Under PCT Article 19 on ___ (if any).

I/we hereby state that I/we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I/we acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I/we hereby claim the benefit under Title 35, United States Code, §119 of any United States provisional patent application, foreign application(s) for patent or inventor's certificate listed below and have also identified below any United States provisional patent application, foreign application for patent or inventor's certificate having a filing date before that of the above-identified application on which priority is claimed: **NOT APPLICABLE.**

I/we hereby claim the benefit under Title 35, United States Code, §120 of any United States patent application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I/we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application: **NOT APPLICABLE.**

I/we hereby appoint the following attorneys/agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith: **George M. Thomas, Reg. No. 22,260; James W. Kayden, Reg. No. 31,532; Scott A. Horstemeyer, Reg. No. 34,183; Stephen R. Risley, Reg. No. 35,659; Jeffrey R. Kuester, Reg. No. 34,367; Daniel J. Santos, Reg. No. 40,158; Daniel R. McClure, Reg. No. 38,962; Robert E. Stachler II, Reg. No. 36,934; David P. Kelley, Reg. No. 17,420; Michael J. Tempel, Reg. No. 41,344; Michael J. D'Aurelio, Reg. No. 40,977; David R. Risley, Reg. No. 39,345; Jon E. Holland, Reg. No. 41,077; Dan R. Gresham, Reg. No. 41,805; M. Paul Qualey, Reg. No. 43,024.**

Please address all telephone calls, in the first instance, to **Jon E. Holland** at telephone number: **(770) 933-9500.**

Address all correspondence to:

**Jon E. Holland
THOMAS, KAYDEN, HORSTEMEYER
& RISLEY, L.L.P.
100 Galleria Parkway, N.W., Suite 1500
Atlanta, Georgia 30339-5948**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statement and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor's Signature: _____ Date: _____

Full Name of First or Sole Inventor: Greg B. Garrison

Residence: 405 Justin Court, Woodstock, Georgia Citizenship: US

Post Office Address: 405 Justin Court
Woodstock, Georgia 30188

Inventor's Signature: _____ Date: _____

Full Name of Second Inventor: _____

Residence: _____ Citizenship: _____

Post Office Address: _____

Inventor's Signature: _____ Date: _____

Full Name of Third Inventor: _____

Residence: _____ Citizenship: _____

Post Office Address: _____
